# Strong Authentication at Fermilab

## Quick Reference Card

**Fermilab Computing Division - http://www.fnal.gov/cd/**
Strong Authentication Documentation at:
http://www.fnal.gov/docs/strongauth/
Quick Reference Card last updated: 09/27/01

## Connect via Kerberized Network Program from UNIX

**The Kerberized network connection programs are located in /usr/krb5/bin. These programs must not prompt for or accept a password! Authenticate locally first!**

| | |
|---|---|
| telnet | **% telnet [options] <host>**<br>Useful Kerberos options (for telnet, rsh and rlogin):<br>**-f** forward existing ticket to host<br>**-F** make forwarded ticket re-forwardable to other hosts<br>**-k <REALM>** specify realm in which to request ticket<br>**-l <username>** specify username on host when different from that on source machine<br>**-N** turn off ticket-forwarding<br>**-x** turn on encryption |
| rsh | **% rsh <host> [options] <command>**<br>Useful options:<br>See telnet |
| rlogin | **% rlogin <host> [options]**<br>Useful Kerberos options:<br>See telnet |
| ftp | **% ftp [options] <host>**<br>Useful Kerberos options:<br>**-f** forward existing ticket to host<br>**-n** disable auto-login; does authentication<br>**-u** disable auto-login; no auto-authentication<br>**protect level** (at **ftp>** propmt) set protection level (**safe** verifies checksum, **private** encrypts data) |
| rcp | **% rcp [options] <file1> <file2>**<br>or<br>**% rcp [options] <file> <directory>**<br>Useful Kerberos options:<br>**-F** forward existing ticket to host<br>**-k <REALM>** specify realm in which to request ticket<br>**-N** turn off ticket-forwarding<br>**-x** turn on encryption |
| ksu | **% ksu [<target_user>]**<br>Useful Kerberos options:<br>**-n <target_principal>** target principal name<br>Useful fact: Can ksu to self (**% ksu .**); no authentication or authorization takes place in this case. |
| ssh or slogin | **% ssh [options] <host> [<commmand>]**<br>or<br>**% slogin [options] <host>**<br>Kerberized ssh (slogin) only! Otherwise you get CRYPTOCard prompt. Useful Kerberos options:<br>**-k** turn off ticket-forwarding |
| scp | **% scp [options] <file1> <file2>**<br>Kerberized scp only! Otherwise you get CRYPTOCard prompt. |

## Connect from Windows or Macintosh

**WRQ is supported by CD at Fermilab, Windows Exceed 7 and Macintosh are not. Authenticate locally before connecting to remote machine.**

| | |
|---|---|
| Windows (WRQ) | Authenticate: **Start > Programs > Reflection > Utilities > Kerberos Manager > Authenticate**<br>Connect via telnet: **Start > Programs > Reflection > Host - UNIX and Digital > File > Open**<br>Connect via FTP: **Start > Programs > Reflection > FTP Client** |
| Windows (MIT Kerberos with Exceed 7) | Authenticate: **Start > Programs > Kerberos Utilities > Leash32 > Action > Get Ticket(s)**<br>Connect via telnet: **Start > Programs > Hummingbird Connectivity v7.0 > HostExplorer > Telnet >** select session file **> Connect** |
| Macintosh (MIT Kerberos, unspecified network client; Newsflash: OS 10.1 kerberos preinstalled) | Authenticate: **Apple menu >Control Panels > Kerberos Control Panel >** select principal **> Get Tickets**<br>Invoke telnet or FTP client to connect (product-dependent) |

## Connect from NonKerberized Machine

**Portal access requires use of a CRYPTOCard (see back side). Commands shown here for UNIX.**

| | |
|---|---|
| ssh or slogin | **% ssh [options] <host>**<br>or<br>**% slogin [options] <host>**<br>Give empty password at first prompt. CRYPTOCard supports ssh only when no command is given. Do not use **-f** and **-n**. Encryption set in config or via **-c <cipher>** option. |
| telnet | **% telnet [options] <host>**<br>Unencrypted! Do not type Kerberos password! |
| ftp | **% ftp [options] <host>**<br>Unencrypted! Do not type Kerberos password! |
| scp | **% scp [options] <file1> <file2>**<br>Encryption set in config or via **-c <cipher>** option. |

## Manage Kerberos Tickets

**These commands manage both Kerberos tickets and AFS tokens when AFS is installed (except kdestroy). In general, only authenticate or change password on local machine. If you must issue password over the network, verify that connection is encrypted!**

| | |
|---|---|
| request tickets | default ticket options: **% kinit**<br>forwardable: **% kinit -f**<br>nonforwardable: **% kinit -F**<br>renewable: **% kinit -r <lifetime>** |
| renew tickets | **% kinit -R** |
| list tickets | showing flags: **% klist -f** |
| destroy tickets | **% kdestroy**<br>Note: this does not destroy AFS token; use:<br>**% unlog** |

## CRYPTOCard Use

**Read the care and use instructions that come with CRYPTOCard!**
**PIN length: 4 to 8 digits.**
**For all CRYPTOCard operations, use ON/OFF to turn the card on to begin, and (optionally) to turn it off when done.**

| | |
|---|---|
| Reset initial PIN | Enter initial PIN, press ENT<br>At prompt “New PIN?”, enter new PIN, press ENT<br>At prompt “Verify”, enter new PIN again, press ENT |
| Reset PIN (general) | Enter old PIN, press ENT<br>At prompt “Fermilab”, press CPIN<br>At prompt “New PIN?”, enter new PIN, press ENT<br>At prompt “Verify”, enter new PIN again, press ENT |
| First use | Enter PIN, press ENT<br>At prompt “Fermilab”, press ENT<br>(terminal) Run ssh, telnet, or ftp to Kerberized host<br>Warning! telnet sessions are not encrypted!<br>(CRYPTOCard) Press CH/MAC<br>Enter challenge from computer screen into card<br>Press ENT to generate response<br>(terminal) Type response from CRYPTOCard |
| General use | Enter PIN, press ENT<br>At prompt “Fermilab”, press ENT to get challenge<br>(terminal) Run telnet, ssh, or ftp to Kerberized host<br>Verify that challenges match<br>(CRYPTOCard) Press ENT to generate response<br>(terminal) Type response from CRYPTOCard |

## Change Kerberos Password

**In general, only change password on local machine. If you must issue password over the network, verify that connection is encrypted!**

| | |
|---|---|
| UNIX | **% kpasswd [<principal_name>]** |
| Windows (WRQ; recommended, CD-supported)) | **Start > Programs > Reflection > Utilities > Kerberos Manager > Tools > Change Password...** |
| Windows (Kerb+Exceed 7; community-supported) | **Start > Programs > Hummingbird Connectivity v7.0 > HostExplorer > Telnet**<br>Then run: **% kpasswd [<principal_name>]** |
| Macintosh (community-supported) | **Apple menu > Control Panels > Kerberos Control Panel >** select principal **> Get Tickets >** click on the ticket **> Change Password** |

## Common Error Messages

**Messages shown in alphabetical order. Message in bold, causes/solutions in plain text underneath.**

**aklog: can’t get afs configuration**
(Users of ssh v1_2_27 or higher) Harmless but misleading. To get rid of, add **AFSRunAklog no** to /etc/sshd_config, restart sshd.

**Cannot contact any KDC for requested realm**
- Firewall blocks KDC request or reply
- DNS failure

**Cannot establish a session with Kerberos administrative server ... preauthentication failed**
Wrong password (most likely)

**Incorrect net address**
NAT or multiple-IP address host. Edit **[libdefaults]** in **krb5.conf**:
- UNIX: **proxy_gateway = <your fixed IP address>**
- Mac: **noaddresses = true**
- WRQ: no solution currently

**KDC policy rejects request**
**KDC can't fulfill requested option**
- Requesting a forwardable ticket for a /root or /admin instance
- Trying to forward an unforwardable ticket, or renew an unrenewable one

**Key version number for principal in key table is incorrect**
- Keytab has changed since service ticket was obtained; to solve, run **% kinit -R** or **% kinit**
- Service key in KDC was changed after keytab file was created; to solve, recreate keytab file on host

**Preauthentication failed while getting initial credentials**
- system clock error > 5 minutes
- wrong password
- user does not have a CRYPTOcard in the host's realm

**Server not found in Kerberos database**
- local hosts file or NIS map gives wrong name for host
- Bad or missing domain_realm mapping in /etc/krb5.conf
- Fermi Kerberos v1_2 bug; to solve, upgrade

WRQ error: **Preauthentication failed (KDC024)**
- Click **Help** for possible causes. Usually realm mismatch, wrong password or system clock error > 5 minutes